Exhibit 10

Engine Installation and Administration

Contents

Engine Installation and Administration.......... 1
About Engine.......... 1
Supported Hardware.......... 1
Network Connectivity.......... 1
Acquire the Engine ISO.......... 2
Install Engine.......... 3
Base System Installation.......... 3
Install on VMware ESXi.......... 4
Registration and Configuration.......... 5
Register the Engine.......... 5
Acquire Sandbox Images.......... 9
Re-registration.......... 10
Delete the Engine.......... 10
Administer the Engine.......... 12
Configuration Tool.......... 12
Network Configuration.......... 13
Reconfigure for DHCP.......... 14
Reconfigure for Static Addressing.......... 15
Update Fully Qualified Domain Name.......... 16
Update On-Premises Manager FQDN.......... 17
Enable the monitoring user.......... 18
Enable Password-Based SSH Authentication.......... 19
Disable Automatic Updates.......... 20
Manual Updates.......... 21
Update Microsoft Product Keys.......... 22
About Hardening.......... 23
Harden the Engine.......... 24

Engine Installation and Administration

This document describes the installation and administration of the Engine in an On-Premises environment.

About Engine

The Engine uses Deep Content Inspection, a unique isolation and inspection environment (sandbox) that simulates an entire host (including the CPU, system memory, and all peripherals) and its operating environment to analyze potentially malicious files. Unknown files, such as applications and documents, and URLs, are submitted from the Manager and other sources. The Engine runs these artifacts in its sandbox and returns the results of its analysis to the Manager, which then displays results.

Supported Hardware

Refer to *Hardware Specifications* on page 25 for details about the hardware certified for use with VMware NSX Network Detection and Response appliances.

Network Connectivity

Domain Names

Assuming that `lastline.example.com` is the FQDN for the Manager, the server hosting the Engine needs to be able to connect to:

- `lastline.example.com` on TCP port 443.
- `user.lastline.example.com` on TCP port 443.
- `log.lastline.example.com` on TCP port 443.
- `update.lastline.example.com` on TCP port 443 and 8443, UDP port 1194,.
- `ntp.lastline.com` on UDP port 123 for time synchronization. It can be replaced with a local NTP server.

Acquire the Engine ISO

Configuration Steps

To install the Engine, you must download the ISO from VMware.

Procedure

Step 1: Refer to your VMware welcome message

Using the information in the VMware welcome email message, point your browser to the User Portal at *https://user.lastline.com/* (https://user.lastline.com/) (for EMEA customers *https://user.emea.lastline.com/* (https://user.emea.lastline.com/)) and then login. For your initial login, use the *Forgot your password?* (https://user.lastline.com/password_reset) link and follow the subsequent instructions.

The licenses you need to run Engine are included in the welcome message. The registration process displays these licenses. Compare the licenses it displays with the provided licenses.

Step 2: Download the ISO

Click the ? icon to access the drop-down help menu. Selected Downloads from the expanded menu. On the *iso-downloads* (https://user.lastline.com/portal#/iso-downloads) page, select the correct ISO and download it to your staging server.

Download the corresponding MD5 file for the ISO. Validate that the `md5sum` of the ISO matches the value in the MD5 file.

Step 3: Prepare the ISO for installation

There are various ways to prepare the ISO. You can burn it to a DVD, create a bootable USB stick, or, if you are using Dell hardware and the iDRAC interface is available on your server, you can use that.

The ISO should be placed on a file share or otherwise made available for a VMware ESXi installation.

Install Engine

The installation process for the Engine consists of three steps. In the first step, the base system is installed. In the second step, basic configuration information is collected and the configuration is applied to the system. In the final step, required data is retrieved from the VMware backend servers.

Base System Installation

Configuration Steps

The Engine uses Ubuntu Server 18.04 (Bionic distribution) as its underlying operating system. Therefore, many of the steps of the installation are similar to the ones required to install Ubuntu Server. Refer to the Ubuntu guide, *Installing Ubuntu 18.04* (https://help.ubuntu.com/18.04/installation-guide/index.html).

Note: Many of the steps involved in a standard Ubuntu installation have been automated and hidden from the Engine Installer.

If you are running an existing installation with appliances based on an earlier Ubuntu release, you should upgrade to a version based on Bionic. To upgrade to Bionic from Xenial, you must first update the Engine to the last version that supports Xenial (see the *release notes* (https://user.lastline.com/releasenotes/) for your specific version, and then follow the instructions on the *linked support article* (https://support.lastline.com/hc/en-us/articles/360051812074)).

Procedure

Step 1: Boot the server from the ISO image

Use the DVD or bootable USB stick you created (or for Dell hardware, the Dell iDRAC interface) to boot the ISO image.

Note: To install the Engine on VMware ESXi, see Install on VMware ESXi.

Step 2: Select the Engine from the boot loader splash screen

Press **[Enter]** to continue.

Step 3: Select keyboard options

The installer needs to localize your keyboard layout and language settings. Select the "Country of origin for the keyboard" and press **[Enter]**. The installer then displays a listing of appropriate keyboard layouts for the selected country. Select the desired "Keyboard layout" and press **[Enter]**.

Step 4: Wait for the system to install and reboot

After the base system is installed successfully, the system will automatically reboot. A login prompt is displayed at the end of the boot process.

Install on VMware ESXi

Prerequisites

Before you install the Engine on VMware ESXi, you must ensure the VM meets the minimum hardware specifications for the class of appliance. See *Hardware Specifications* on page 25 for details.

Configuration Steps

Using the VMware ESXi vSphere client, create a new virtual machine and configure it to meet the requirements of the Engine.

Procedure

Step 1: Access the Engine ISO

Navigate to Configuration→Storage. Right-click on the relevant datastore and select Browse Datastore from the drop-down menu. Select the Engine ISO and click the Upload icon.

Step 2: Create a new virtual machine

Navigate to File→New→Virtual Machine. In the Create New Virtual Machine pop-up, perform the following:

- Create a Custom VM and specify its Name.
- Select the destination Storage for the VM.
- If supported, select the correct Virtual Machine Version.
- Set the Guest Operating System to Linux then select Ubuntu Linux (64 bit).
- Configure the Engine with 20 sockets × 1 core (unless required otherwise by your VMware ESXi license).
- Set the VN Memory to 96 GB.
- At least one Network NIC is used for the management IP address.

- Define the SCSI Controller.
- Create a new disk and set its size to 1 TB. The Engine requires a second similar sized disk.

You can add more hardware to the VM after the initial configuration. Select the check-box for Edit the virtual machine settings before completion. Use this feature to add more storage to the VM.

Set the New CD/DVD to point at the Engine ISO (Step 1 (page 4)). Ensure it is set to Connect at power on.

Step 3: Expose CPU virtualization to the guest operating system

Right-click on the virtual machine and select Edit Settings. Expand the CPU category and select Expose hardware assisted virtualization to the guest OS. Click OK.

Step 4: Start the VM

VMware ESXi boots the ISO image.

The boot process then proceeds as in Base System Installation, Step 2 (page 3) through Step 4 (page 4).

Registration and Configuration

Prerequisites

Before you can configure Engine for an On-Premises installation, you must have previously installed and configured the Manager. The Manager must be on-line and reachable.

For a hosted installation using the NSX Cloud, the User Portal must be accessible at *https://user.lastline.com/* (https://user.lastline.com/) (for EMEA customers *https://user.emea.lastline.com/* (https://user.emea.lastline.com/)).

Configuration Steps

To register and apply the software configuration to the Engine, you must login to the server console.

Register the Engine

Procedure

Step 1: Login to the server console

Login to the console using the username `lastline` and its current password.

Important: The default user is `lastline` and its password is `lastline`. For your security and protection, you should change the default password. Your password selection must meet the requirements specified on the *`passwd` command man page* (https://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

Step 2: Start the configuration and registration process

Execute the `lastline_register` command, which will start the guided configuration and registration process.

```
lastline@lastline-engine:~$ lastline_register
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step Result

The `lastline_register` command first validates the server. If its hardware is not sufficient to run the Engine, the command terminates with an error message. Should this occur, contact *VMware Support* (https://my.vmware.com/group/vmware/get-help) for further guidance.

Step 3: Select the primary network interface and network address

The registration process prompts you to select the "`Primary network interface`". It presents a list of interfaces discovered during the validation process. Select the interface that is used by the server to communicate with the other hosts on the network.

Then you are prompted to select how the server will obtain its network address. Your choice is "`Obtain via DHCP`" or "`Enter static address`".

If you select "`Enter static address`", you are prompted to provide an IP address to assign to the interface, its netmask, gateway IP address, and domain name server IP address.

To continue, select `<Ok>` or press **[Enter]**.

Step 4: Provide the address of the Manager

The registration process prompts you for the FQDN of the On-Premises Manager appliance. For example, if its domain name is `lastline.example.com`, then this name should be provided.

If the Manager does not have a FQDN assigned to it (or the DNS server is unable to resolve its domain name), then its IP address must be provided instead.

Note: If the Manager is deployed in an active-standby configuration, you must use the configured virtual IP address, either taken from DNS or using the address directly. The Engine will go into an Error state if this is not correctly configured.

In addition to the FQDN of the Manager, the following names should have also been registered as aliases and mapped to the same IP address:

- `user.lastline.example.com`
- `update.lastline.example.com`
- `log.lastline.example.com`

To continue, select `<Ok>` or press **[Enter]**.

Step Result

The registration process attempts to contact the Manager. Upon success, it displays the FQDN (if available) and IP address of the Manager and prompts you to accept the mapping it discovered.

To continue, select `<Ok>` or press **[Enter]**.

Step 5: Configure an NTP server

The Network Time Protocol (NTP) is used to set the correct time for the Engine. Enter the address of the NTP server. This address can be a FQDN or an IP address.

Note: The selected NTP server must be reachable over UDP port 123. Unless you must use a specific NTP server, use the default value, `ntp.lastline.com`.

To continue, select `<Ok>` or press **[Enter]**.

Step Result

The network configuration is tested to check for connectivity to the VMware backend; to either the NSX Cloud or, for an On-Premises installation, Manager. This test may take a while.

Step 6: Provide a network for local communication

The Engine employs a number of *Docker* (https://docs.docker.com/) containers to provide its services. These containers require an internal network to use for communication. By default, this network uses `169.254.64.0/20`, a portion of the *IPv4 link-local address space* (https://tools.ietf.org/html/rfc3927). This network does not need to be reachable from outside services or hosts. It also must not overlap with any of your existing network address ranges.

For most installations you should accept the default and continue. However, if you are already using the `169.254.0.0/16` address space, you must provide a valid IPv4/20 (or larger) network that can be used for local communication. This network must be in the format `A.B.C.0/X`, for example, `169.254.64.0/20`, `240.0.0.0/16`, `10.0.0.0/12`, or `192.168.0.0/16`.

To continue, select `<Ok>` or press **[Enter]**.

Step 7: Accept Manager SSL certificate

The registration process attempts to verify the SSL certificate for the Manager. Because the appliances use self-signed SSL certificates, the verification check fails. The certificate is displayed and you are prompted to trust it.

Select `<Yes>` to continue the registration.

Step 8: Enter your Windows and Office Product Keys

The Engine uses Microsoft Windows operating systems and Microsoft Office applications in the sandbox to perform its analysis of potentially malicious downloads and attachments. You are required to have valid Product Keys for Windows and for Office before you can complete the registration of the Engine. VMware is required to ensure the validity of your license. Therefore the registration process prompts you for these Product Keys.

Note: Microsoft always provides a Product Key with its software in the format `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`. The Engine accepts the Microsoft Product Key entry in the following formats:

- `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
- `XXXXX XXXXX XXXXX XXXXX XXXXX`
- `XXXXXXXXXXXXXXXXXXXXXXXXX`

The registration process prompts you for your Windows Product Key. Enter it at the Microsoft Windows Product Key prompt using one of the formats above.

To continue, select `<Ok>` or press **[Enter]**.

The registration process prompts you for your Office Product Key. Enter it at the Microsoft Office Product Key prompt using one of the formats above.

To continue, select `<Ok>` or press **[Enter]**.

Step 9: Enter your VMware username and password

As the first stage to applying your license to the Engine you are prompted for your VMware username. Enter your username and then select `<Ok>` or press **[Enter]**.

Note: This is your User Portal username. It is not the same username used in Step 1 (page 5).

For this step to succeed, you must have login access to the User Portal (see Acquire the Engine ISO, Step 1 (page 2)).

Enter your VMware password and then select `<Ok>` or press **[Enter]**.

Step 10: Select the correct license

If the credentials you provided are valid, the registration process displays a list of the available license keys. Use the **[UP]** and **[DOWN]** keys to select the correct license.

Note: If there are no valid licenses associated with your credentials or your list of license keys is not retrieved correctly, contact *VMware Support* (https://my.vmware.com/group/vmware/get-help). Provide the error message the registration process displayed in your request.

To continue, select `<Ok>` or press **[Enter]**.

Step Result

The registration process displays a prompt: "`Registration completed successfully`".

To continue, select `<Ok>` or press **[Enter]**.

Configuration Result

The registration process runs some tests to check hardware compatibility. The configuration is then applied to the machine. This process may take a while (20-40 minutes) depending on your network connectivity and system characteristics.

After the completed prompt is displayed, select `<Ok>` or press **[Enter]** to exit from the registration process.

Acquire Sandbox Images

Configuration Steps

Engine must download the images used by the malware analysis sandbox component from the VMware backend servers. The image files consist of approximately 30 GB of compressed data. This step might take several hours, depending on the available network bandwidth.

Note: The Engine acquires the sandbox images from the Manager.

Procedure

Step 1: Download the sandbox images

Run the `lastline_download_engine_data` command.

```
lastline@lastline-engine:~$ lastline_download_engine_data
```

Step 2: Confirm the download

Use the `-f` option to the `lastline_download_engine_data` command to confirm that you successfully acquired all the sandbox images.

```
lastline@lastline-engine:~$ lastline_download_engine_data -f
```

Re-registration

Configuration Steps

If the Engine needs to be replaced or reinstalled, the existing appliance needs to be deregistered first before your new registration will succeed.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the Manager Web UI.

Step 2: Access the Appliances page

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Admin]** from left sidebar menu. For most users, the Appliances page is displayed by default.

Step 3: View the appliance status

On the Appliances page, click the Status tab.

Step 4: *Optional:* Select an appliance

If no appliance is currently selected, click the **[Appliance: None Selected]** link. From the Select Appliance pop-up tick the box for the appliance you want to use, then click **[SELECT APPLIANCE]**.

Step 5: Deregister the existing Engine

To deregister a Engine, click the **[⚙]** button and select Deregister from the drop-down menu.

Step 6: Register the reinstalled Engine

To replace or reinstall a Engine, you must run the `lastline_register` command again from the server console (see *Register the Engine* on page 5).

Delete the Engine

Prerequisites

Before you can successfully delete the Engine from the User Portal it must be offline. The easiest way to do this is to login to the appliance and shut it down.

Configuration Steps

To delete the Engine, it needs to be offline and deregistered.

Procedure

Step 1: Shutdown the appliance

Login to the server console of the Engine and shut down the operating system.

```
lastline@lastline-engine:~$ shutdown now
```

Step 2: Login to the Web UI

Using your Web browser, login to the Manager Web UI.

Step 3: Access the Appliances page

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Admin]** from left sidebar menu. For most users, the Appliances page is displayed by default.

Step 4: View the appliance status

On the Appliances page, click the Status tab.

Step 5: Deregister the Engine

Click the **[⚙]** button and select Deregister from the drop-down menu.

Step 6: Delete the appliance

Click the Overview tab to return to the initial view. In the appliances listing, the STATUS of the Engine must be DEREGISTERED.

In the ACTIONS column, click the **[QUICK LINKS]** icon and select Delete. A confirmation pop-up is displayed. Click **[DELETE APPLIANCE]** to dismiss the pop-up. The Engine is permanently deleted.

Administer the Engine

The Engine was developed to require as little maintenance and administration as possible.

The following topics describe how to customize and configure some of the advanced features of the Engine.

Configuration Tool

Configuration Steps

Use the VMware NSX Network Detection and Response configuration tool, `lastline_setup`, to administer and manage the Engine.

Procedure

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-engine:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step 2: Run the help option

To view all the supported options, type `help`.

```
-> help
Documented commands (type help <topic>):
========================================
EOF                        help                           ntp_server
appliance_state            llama_images_server_override   ntp_servers
appliance_uuid             manager                        save
disable_support_channel    monitoring_user_password       show
edit                       network
exit                       new_monitoring_user_password
```

Tip: For any option, type the first few unique characters of its name then type **[Tab]**. The `lastline_setup` command will auto-complete the name for you.

Step 3: View help details

To view a detailed description of individual options, type `help` *`topic`*, where *`topic`* is the name of a specific option.

```
-> help network
 network <variable> [<new-value>]
        Get/set network settings.
            network interface <iface>: interface used for network access
            network method dhcp|static: use DHCP or static IP address
                configuration for network access
        When static configuration is used, these values must also be set:
            network address <address>: IPv4 address of the interface
            network netmask <netmask>: dotted-quad netmask for the address
            network gateway <gateway>: default gateway for network access; if
                specified value is -, set gateway to None
            network dns_nameservers <nameserver> ...: space-separated list of
                DNS nameservers, if specified value is -, set dns_nameservers to
                None
```

Step 4: Exit the configuration tool

To quit from the configuration tool without saving your changes, type `exit`.

```
-> exit
lastline@lastline-engine:~$
```

Troubleshooting

Important: If you encounter an error running any of the `lastline_setup` command options, make a note of the error message returned and contact *VMware Support* (https://my.vmware.com/group/vmware/get-help).

Network Configuration

Configuration Steps

You can easily change the network configuration of the Engine. This may be needed if its assigned IP address changes (for example, upon a reconfiguration of the network).

Reconfigure for DHCP

Configuration Steps

To enable a network configuration using DHCP, use the `network` option of the `lastline_setup` command.

Procedure

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-engine:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step 2: Check the network settings

To check the current network settings, type `network`.

```
-> network
network dns_nameservers = 8.8.8.8 8.8.4.4
network gateway = 10.0.2.2
network netmask = 255.255.255.0
network address = 10.0.2.15
network interface = eth0
network method = static
```

Step 3: Enable DHCP configuration for network access

To enable DHCP addressing, type `network method dhcp`.

```
-> network method dhcp
network method = dhcp  # changed; original value: static
```

Step 4: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Reconfigure for Static Addressing

Configuration Steps

To enable a network configuration using a static IP, you must provide values for the address, netmask, gateway, and dns_nameservers parameters. Use the `network` options of the `lastline_setup` command to make these changes.

Procedure

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-engine:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step 2: Check the network settings

To check the current network settings, type `network`.

```
-> network
network interface = eth0
network method = dhcp
```

Step 3: Enable static configuration for network access

To enable a static IP address, type `network method static`.

```
-> network method static
network method = static  # changed; original value: dhcp
```

Step 4: Set the network address

To set the IP address, type `network address` *`ip_address`*. Use an IPv4 address of four octets.

```
-> network address 10.0.2.15
network address = 10.0.2.15  # changed; original value:
```

Step 5: Set the netmask

To set the netmask, type `network netmask` *`netmask`*. Use an IPv4 netmask of four octets.

```
-> network netmask 255.255.255.0
```

```
network netmask = 255.255.255.0  # changed; original value:
```

Step 6: Set the gateway address

To set the gateway IP address, type `network gateway` *`ip_address`*. Use an IPv4 address of four octets.

```
-> network gateway 10.0.2.2
network gateway = 10.0.2.2  # changed; original value:
```

Step 7: Set the DNS server address(es)

To set the DNS server IP address, type `network dns_nameservers` *`ip_address`* `[`*`ip_address`*`]`. Use an IPv4 address of four octets for each address.

```
-> network dns_nameservers 10.2.1.1 10.2.2.1
network dns_nameservers = 10.2.1.1 10.2.2.1  # changed; original value:
```

Step 8: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Update Fully Qualified Domain Name

Configuration Steps

You can update the FQDN of the Engine.

Procedure

Step 1: Login to the console

Login to the console using the username `lastline` and its current password.

Step 2: Run the registration process with the change FQDN option

Execute the `lastline_register` command, providing the new local FQDN for the Engine in its arguments.

```
lastline@lastline-engine:~$ lastline_register --change-local-fqdn new_engine.lastline.example.com
```

Note: If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Update On-Premises Manager FQDN

Configuration Steps

If you had selected "Use On-Premises Manager" during the registration and configuration of the Engine and the FQDN of the Manager changes, you must update the FQDN information to ensure your appliances can continue to successfully communicate.

Important: This process does not allow you to move appliances from one Manager to another.

If the Manager is deployed in an active-standby configuration, you must use the configured virtual IP address, either taken from DNS or using the address directly.

Procedure

Step 1: Login to the console

Login to the console using the username `lastline` and its current password.

Step 2: Run the registration process

Execute the `lastline_register` command with the `change-active-manager-fqdn` option, providing the new FQDN for the Manager as its argument.

```
lastline@lastline-engine:~$ lastline_register --change-active-manager-fqdn \
new_manager.lastline.example.com
```

Note: If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

If the Manager is using a self-signed SSL certificate, the appliance needs to be configured to trust the new SSL certificate to ensure all communication succeeds. Use the following commands instead:

```
lastline@lastline-engine:~$ lastline_register -C --change-active-manager-fqdn \
new_manager.lastline.example.com
lastline@lastline-engine:~$ lastline_test_appliance --auto-fix network:master_api_query
lastline@lastline-engine:~$ lastline_apply_config -f
```

If the Active Manager IP address is assigned statically, the following command can be used to update `/etc/hosts` to point to its new address:

```
lastline@lastline-engine:~$ lastline_register --change-active-manager-ip 192.20.24.42
```

You can combine both options into a single command:

```
lastline@lastline-engine:~$ lastline_register --change-active-manager-fqdn \
new_manager.lastline.example.com --change-active-manager-ip 192.20.24.42
lastline@lastline-engine:~$ lastline_test_appliance --auto-fix network:master_api_query
lastline@lastline-engine:~$ lastline_apply_config -f
```

Enable the monitoring user

Configuration Steps

The Engine has a monitoring user who can access the system using console or via SSH (password only without using the SSH key). To enable the monitoring user, use the `monitoring_user_password` option of the `lastline_setup` command.

Procedure

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-engine:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step 2: Enable the monitoring user

To enable the monitoring user, type `monitoring_user_password` *`password`*.

```
-> monitoring_user_password s3cretP4ssw0rd
```

Your password selection must meet the requirements specified on the *passwd command man page* (https://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

If you type the `monitoring_user_password` option without an argument, the status of the monitoring user is displayed.

```
-> monitoring_user_password
monitoring_user_password: enabled; pending password change
```

To subsequently disable the monitoring user account, use the dash (`-`) argument:

```
-> monitoring_user_password -
```

Step 3: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Configuration Result

Once the monitoring user is enabled, you can SSH to the Engine using that account:

```
server# ssh monitoring@ip_appliance
monitoring@ip_appliance's password:

...

monitoring@lastline-manager:~$
```

Enable Password-Based SSH Authentication

Configuration Steps

The Engine supports specifying users who can access the system using console or via SSH (password only without using the SSH key). To enable existing users to authenticate with password-based SSH use the `enable_additional_password_auth_ssh_usernames` option of the `lastline_setup` command.

Procedure

Step 1: Start the configuration tool

Execute the `lastline_setup` command.

```
lastline@lastline-engine:~$ lastline_setup
```

If you are prompted for the `sudo password`, use the password for the default `lastline` user account.

Step 2: Enable password-based SSH authentication for one or many users

To enable password-based SSH authentication, type `enable_additional_password_auth_ssh_usernames` *`username`*.

```
-> enable_additional_password_auth_ssh_usernames ghopper
```

Multiple users can be specified as a comma-separated list, such as: `enable_additional_password_auth_ssh_usernames` *`ghopper,aturing`*.

Note: The users need to exist before enabling password-based SSH authentication.

Your password selection must meet the requirements specified on the *`passwd` command man page* (https://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

If you type the `enable_additional_password_auth_ssh_usernames` option without an argument, the list of users who can use password-based SSH authentication is displayed.

```
-> enable_additional_password_auth_ssh_usernames
enable_additional_password_auth_ssh_usernames = ghopper
```

To remove all users (with the exception of the monitoring user, if enabled), use the dash (`-`) argument:

```
-> enable_additional_password_auth_ssh_usernames -
```

Step 3: Save the configuration

After you provide all the required parameters, save your configuration.

```
-> save
```

Configuration Result

Once the user has been added, you can SSH to the Engine using that account:

```
server# ssh ghopper@ip_appliance
ghopperg@ip_appliance's password:

...

ghopper@lastline-manager:~$
```

Disable Automatic Updates

Configuration Steps

VMware periodically releases appliance updates or hotfixes. By default, automatic updates are enabled on newly installed appliances. As long as the appliance has automatic updates enabled, these updates and fixes will transparently be applied to the system.

If you prefer to manually update the Engine, follow these steps to disable automatic updates.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the Manager Web UI.

Step 2: Access the Appliances page

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Admin]** from left sidebar menu. For most users, the Appliances page is displayed by default.

Step 3: View the appliance configuration

On the Appliances page, click Configuration tab.

Step 4: *Optional:* **Select an appliance**

If no appliance is currently selected, click the **[Appliance: None Selected]** link. From the Select Appliance pop-up tick the box for the appliance you want to use, then click **[SELECT APPLIANCE]**.

Step 5: Access the SYSTEM tab

Click the SYSTEM tab.

Step 6: Disable automatic updates

Toggle the Auto Update button to **[DISABLED]**.

Step Result

The appliance will no longer automatically apply updates and hotfixes when released by VMware. You must apply those manually.

Manual Updates

Configuration Steps

If you have disabled automatic updates for your appliances you must apply updates and hotfixes manually.

Follow these steps to manually update an appliance.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the Manager Web UI.

Step 2: Access the Appliances page

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Admin]** from left sidebar menu. For most users, the Appliances page is displayed by default.

Step 3: View the appliance status

On the Appliances page, click the Status tab.

Step 4: *Optional:* Select an appliance

If no appliance is currently selected, click the **[Appliance: None Selected]** link. From the Select Appliance pop-up tick the box for the appliance you want to use, then click **[SELECT APPLIANCE]**.

Step 5: Update the selected appliance

To update an appliance, click the **[⚙]** button and select Upgrade from the drop-down menu.

Update Microsoft Product Keys

Configuration Steps

You may want to change the Microsoft Product Keys you provided, or you may need to enter the keys when upgrading from an earlier version of the Engine (as, during auto-upgrade, the `lastline_register` command is not invoked manually).

To avoid blocking reconfigurations, `lastline_register` does not prompt for Microsoft Product Keys after the initial installation. To update the Product Keys, provide the `--configure-microsoft-product-keys` option when you launch the `lastline_register` command.

Procedure

Step 1: Login to the server console

Login to the console using the username `lastline` and its current password.

Important: The default user is `lastline` and its password is `lastline`. For your security and protection, you should change the default password. Your password selection must meet the requirements specified on the *`passwd` command man page* (https://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

Step 2: Start the registration process

To update the Microsoft Product Keys, provide the `--configure-microsoft-product-keys` option.

```
lastline@lastline-engine:~$ lastline_register --configure-microsoft-product-keys
```

The `lastline_register` command will validate the server and then proceed to prompt you through the registration process. For most prompts, select `<Ok>` or press **[Enter]** to continue.

Step 3: Enter your Windows and Office Product Keys

The Engine uses Microsoft Windows operating systems and Microsoft Office applications in the sandbox to perform its analysis of potentially malicious downloads and attachments. You are required to have valid Product Keys for Windows and for Office before you can complete the registration of the Engine. VMware is required to ensure the validity of your license. Therefore the registration process prompts you for these Product Keys.

Note: Microsoft always provides a Product Key with its software in the format `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`. The Engine accepts the Microsoft Product Key entry in the following formats:

- `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
- `XXXXX XXXXX XXXXX XXXXX XXXXX`
- `XXXXXXXXXXXXXXXXXXXXXXXXX`

The registration process prompts you for your Windows Product Key. Enter it at the Microsoft Windows Product Key prompt using one of the formats above.

To continue, select `<Ok>` or press **[Enter]**.

The registration process prompts you for your Office Product Key. Enter it at the Microsoft Office Product Key prompt using one of the formats above.

To continue, select `<Ok>` or press **[Enter]**.

Step 4: Complete the registration process

After the completed prompt is displayed, select `<Ok>` or press **[Enter]** to exit from the registration process.

About Hardening

During the development process, steps were taken to lock down the Engine by default to help reduce any attack surfaces. These include:

- **Default Applications** — All unnecessary applications included in the base *Ubuntu server* (https://www.ubuntu.com/server) build have been removed from the system. What remains are the libraries and applications necessary for the normal functioning, routine maintenance, and troubleshooting of the Engine.

- **Default Firewall** — The Engine image comes with *Uncomplicated FIrewall* (https://wiki.ubuntu.com/UncomplicatedFirewall) (UFW) installed and configured to restrict inbound access to the system.
- **Security Patches** — The system will install daily OS security updates by default. You can *disable automatic updates* (see page 20).
- **Least privilege** — VMware has taken care to ensure a paradigm of least privilege regarding the permissions of services and file system access.
- **Secure SSH** — SSH is configured to use certificate-based authentication by default.
- **TLS encryption** — Communications between the appliances are TLS encrypted.

Harden the Engine

Configuration Steps

We recommend the following guidelines for hardening the Engine after installation. These steps are not required, but they will allow you to further restrict access to your VMware NSX Network Detection and Response appliances.

Procedure

Step 1: Change the default user password

The default user is `lastline`. Your password selection must meet the requirements specified on the *`passwd` command man page* (https://manpages.ubuntu.com/manpages/precise/man1/passwd.1.html).

Step 2: Use sudo for elevated privileges

Enabling the root user is strongly discouraged. Instead you should use the `sudo` command when you need elevated privileges. This ensures proper logging and auditing of activity on the appliance.

If you wish to further refine which commands a specific user can run, refer to the following pages on *ubuntu.com* (https://www.ubuntu.com/) to learn how to configure and use the `sudo` command: *RootSudo* (https://help.ubuntu.com/community/RootSudo), *Sudoers* (https://help.ubuntu.com/community/Sudoers), and *sudo manpage* (http://manpages.ubuntu.com/manpages/trusty/man8/sudo_root.8.html).

Step 3: Configure the support channel

VMware Support leverages the support channel to ensure your systems are functioning as intended. Should you wish to disable this, we recommend you re-enable it prior to submitting a support ticket. This will allow VMware Support to investigate issues and respond with a resolution more rapidly.

You disable/enable the support channel with the `disable_support_channel` option of the *`lastline_setup` command* (see page 12).

Step 4: Configure the monitoring user

By default, the `monitoring` user is disabled. You enable the monitoring user using the `monitoring_user_password` option of the `lastline_setup` command. For logging and auditing purposes, we recommend that you do not share the `monitoring` user with multiple users.

Refer to *Enable the monitoring user* (see page 18) for further information about enabling the monitoring user.

Step 5: Use per-user key-based SSH authentication

By default, the Engine is configured to utilize key-based authentication. We recommend that individual user accounts are configured on the appliance for anyone needing to carry out administrative tasks. Refer to this article on *SSH.com* (https://www.ssh.com/ssh/key/) for further information about key-based authentication.

Step 6: Change iDRAQ password

If you have installed the Engine on one of the recommended Dell systems, these systems include an iDRAQ interface for remote management. The iDRAQ interface is configured with a default password. This password must be changed to prevent unauthorized access to the system console.

Hardware Specifications

The hardware certified for use with VMware NSX Network Detection and Response appliances is listed below:

Dell Hardware

Supported Dell Hardware

✅ **Manager**

Server Model	Dell PowerEdge R450
CPU Type	• Recommended: Intel® Xeon® Silver 4314 • Minimum: Intel® Xeon® Silver/Gold/Platinum 2.0 GHz, 12 cores
CPU Quantity	1 CPU
Minimum RAM	96 GB

Manager

RAID Controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)
RAID Configuration	RAID 10 **Note:** If the Dell website does not allow RAID 10 configuration from factory, purchase the server with RAID unconfigured and then manually create a RAID 10 virtual volume before software installation.
Persistent Storage	Recommended: 4 × 4 TB HDDs
Additional Network Card	None
Redundant Power Supply	Recommended for reliability
iDRAC9 Enterprise	Recommended for remote management and installation

Data Node

Server Model	Dell PowerEdge R450
CPU Type	• Recommended: Intel® Xeon® Silver 4314 • Minimum: Intel® Xeon® Silver/Gold/Platinum 2.0 GHz, 12 cores
CPU Quantity	1 CPU
Minimum RAM	96 GB
RAID Controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)
RAID Configuration	RAID 10 **Note:** If the Dell website does not allow RAID 10 configuration from factory, purchase the server with RAID unconfigured and then manually create a RAID 10 virtual volume before software installation.
Persistent Storage	Recommended: 4 × 2 TB 10k RPM HDDs
Additional Network Card	None
Redundant Power Supply	Recommended for reliability
iDRAC9 Enterprise	Recommended for remote management and installation

Engine

Server Model	Dell PowerEdge R450
CPU Type	• Recommended: Intel® Xeon® Silver 4314 • Minimum: Intel® Xeon® Silver/Gold/Platinum 2.0 GHz, 12 cores, with Intel Virtualization Technology (VT-x) and Intel VT-x with Extended Page Tables (EPT)

☑ Engine

CPU Quantity	1 CPU
Minimum RAM	128 GB Recommended: 4 GB per CPU virtual core
RAID Controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)
RAID Configuration	RAID 1
Persistent Storage	Minimum: 2 × 1 TB HDDs
Additional Network Card	None
Redundant Power Supply	Recommended for reliability
iDRAC9 Enterprise	Recommended for remote management and installation

☑ Sensor — 1G Networks

Server Model	Dell PowerEdge R450
CPU Type	• Recommended: Intel® Xeon® Silver 4314 • Minimum: Intel® Xeon® Silver/Gold/Platinum 2.0 GHz, 12 cores
CPU Quantity	1 CPU
Minimum RAM	64 GB
RAID Controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)
RAID Configuration	RAID 1
Persistent Storage	Minimum: 2 × 1 TB HDDs
Additional Network Card	Intel i350 Quad Port 1GbE
Redundant Power Supply	Recommended for reliability
iDRAC9 Enterprise	Recommended for remote management and installation

☑ Sensor — 10G Networks

Server Model	Dell PowerEdge R450
CPU Type	• Recommended: Intel® Xeon® Silver 4314 • Minimum: Intel® Xeon® Silver/Gold/Platinum 2.0 GHz, 12 cores
CPU Quantity	2 CPUs
Minimum RAM	192 GB

✅ Sensor — 10G Networks

RAID Controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)
RAID Configuration	RAID 1
Persistent Storage	Minimum: 2 × 1 TB HDDs
Additional Network Card	Intel X710 Dual Port 10GbE
Redundant Power Supply	Recommended for reliability
iDRAC9 Enterprise	Recommended for remote management and installation

Previously Supported Dell Hardware

The following Dell hardware are no longer supported.

🚫 Manager

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 12 threads/cores)
CPU Quantity	1 CPU
Minimum RAM	64 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	4 × 2 TB 7.2K RPM SATA 6Gbps 3.5in
Power Supply	Dual Hot-plug Power — Optional
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 Data Node

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 24 threads/cores)
CPU Quantity	1 CPU
Minimum RAM	64 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller

🚫 Data Node

Minimum Persistent Storage	2 × 1 TB SATA HDD
Power Supply	Dual Hot-plug Power — Optional
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 Engine

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 20 threads/cores)
CPU Quantity	1 CPU
Minimum RAM	96 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	2 × 1 TB SATA HDD
Power Supply	Dual Hot-plug Power — Optional
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 Sensor — 1G Networks

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 20 threads/cores)
CPU Quantity	1 CPU
Minimum RAM	32 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	2 × 1 TB SATA (7.2K RPM) HDD
Power Supply	Dual Hot-plug Power — Optional
Network Card	Intel Ethernet I350 Quad-Port 1Gb Server Adapter
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 Sensor — 10G Networks

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 20 threads/cores)
CPU Quantity	2 CPUs
Minimum RAM	128 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	2 × 1 TB SATA (7.2K RPM) HDD
Power Supply	Dual Hot-plug Power — Optional
Network Card	Intel Ethernet X710-DA2 10Gbps network card
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 All-In-One

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 20 threads/cores)
CPU Quantity	2 CPUs
Minimum RAM	128 GB ECC RAM
RAID Controller	HW RAID10
RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	4 × 2 TB 7.2K RPM SATA 6Gbps 3.5in
Power Supply	Dual Hot-plug Power — Optional
Network Card	Intel Ethernet X710-DA2 10Gbps network card
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

🚫 Analyst

Server Model	Dell PowerEdge R440
Chassis Type	Chassis with Hot-plug Hard Drives
CPU Type	Intel® Xeon® Silver 4114 — or better (minimum 12 threads/cores)
CPU Quantity	1 CPU
Minimum RAM	96 GB ECC RAM
RAID Controller	HW RAID10

🚫 Analyst

RAID Configuration	• PERC H730P+ RAID Controller • PERC H740P RAID Controller • PERC H750 RAID Controller
Minimum Persistent Storage	4 × 2 TB 7.2K RPM SATA 6Gbps 3.5in
Power Supply	Dual Hot-plug Power — Optional
iDRAC9 Enterprise	Optional
ProSupport Service Plan	Optional

HPE Hardware

Manager

HPE ProLiant DL360 Gen10:

- Intel® Xeon® Silver 4114 2.2GHZ
- 64 GB RAM
- 4 × 2 TB in RAID 10 (6 Gbps SATA)
- On-board NIC
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

Data Node

HPE ProLiant DL360 Gen10:

- Intel® Xeon® Silver 4114 2.2GHZ
- 64 GB RAM
- 4 × 2 TB in RAID 10 (SAS 10K RPM)
- On-board NIC
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

Engine

HPE ProLiant DL360 Gen10:

- Intel® Xeon® Silver 4114 2.2GHZ
- 96 GB RAM
- 2 × 2 TB HDDs in RAID 1 (6 Gbps SATA)
- On-board NIC
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

Sensor — 1G Networks

HPE ProLiant DL360 Gen10:

- Intel® Xeon® Silver 4114 2.2GHZ
- 32 GB RAM
- 2 × 2 TB HDDs in RAID 1 (6 Gbps SATA)
- Intel I350 Quad port (or HPE 366T)
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

Sensor — 10G Networks

HPE ProLiant DL360 Gen10:

- 2 × Intel® Xeon® Silver 4114 2.2GHZ
- 128 GB RAM
- 2 × 2 TB HDDs in RAID 1 (6 Gbps SATA)
- Intel X710-DA2
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

Analyst

HPE ProLiant DL360 Gen10:

- 2 × Intel® Xeon® Silver 4114 2.2GHZ
- 128 GB RAM
- 2 × 2 TB HDDs in RAID 1 (6 Gbps SATA)
- On-board NIC
- HPE Smart Array P408i-p SR Gen10 storage controller
- iLO advanced license

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com